Jim Gildersleeve

1. You can catch many implementation bugs, but if there is something wrong with the design, it is unlikely that you will find an error until it happens.
2. With a precise description of software design, you can find more subtle bugs with tools. It also forces designers to think more about the design and avoid oversight.
3. TLA+ is a language that enables precise description of software design. PlusCal was needed because it was much more expressive
4. Formal methods are useful for more than just avionics and healthcare. Any software can Formal methods to guarantee that it does what it says it does more confidently. Amazon used Formal methods to assert that DynamoDB did have strong consistency. It also does not take a ton of training and effort to learn. The paper found that engineers were able to learn TLA+ in two to three weeks.
5. The two key correctness properties are safety and liveness. Safety is a statement of what a system can do and what it should not do. Liveness is about what the system will do in some amount of time.
6. Amazon’s precise design model makes it easy for them to quickly change things and see if it works. They have prevented the introduction of new bugs into production code by verifying it using formal methods ahead of time. They have also used formal methods to verify that some optimizations would not introduce any bugs that they previously would never attempt to implement.
7. TLA+ is not very useful for nonfunctional requirements. TLA+ and other tools can detect actual logic errors, but it cannot determine anything about how well something is completed.
8. Chris Newcombe was not pleased with the quality of several distributed systems that he had designed. Zave, who used Alloy to develop a concurrent algorithm that won the 10-year test of time award, inspired Newcombe. He did not use Alloy because he wanted a language that would better describe system states.
9. TLA+ was used for some cache-coherency protocols and the Paxos algorithm.
10. Tim Rath felt the need for formal methods because he found that his informal proofs missed some very subtle problems. He used formal methods to verify a small complicated part of the dynamoDB algorithm, then worked out to a bigger fault-tolerant algorithm. He found a bug that would result in some lost data.
11. Amazon also used TLA+ to find a critical bug in one of AWS’s most important new distributed algorithms, develop a major protocol optimization that reduced write latency, and also for designing schemas for databases